TRAITÉ COOPÉRATION EN MATIÈRE BREVETS

PCT

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

(chapitre II du Traité de coopération en matière de brevets)

10/534855

Référence du dossier du déposant ou du mandataire	POUR SUITE À DONNER voir formulaire PCT/IPEA/416	
Demande internationale No. PCT/FR 03/03309	Date du dépôt international *(jour/mois/année)* 05.11.2003	Date de priorité *(jour/mois/année)* 14.11.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F17/50		
Déposant EADS TELECOM et al.		

1. Le présent rapport est le rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international en vertu de l'article 35 et transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.
3. Ce rapport est accompagné d'ANNEXES, qui comprennent :
   a. ☒ un total de *(envoyées au déposant et au Bureau international)* 6 feuilles, définies comme suit :
      - ☐ les feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou des feuilles contenant des rectifications autorisées par la présente administration (voir la règle 70.16 et l'instruction administrative 607).
      - ☐ des feuilles qui remplacent des feuilles précédentes, mais dont la présente administration considère qu'elles contiennent une modification qui va au-delà de l'exposé de l'invention qui figure dans la demande internationale telle qu'elle a été déposée, comme il est indiqué au point 4 du cadre n° I et dans le cadre supplémentaire.

   b. ☐ *(envoyées au Bureau international seulement)* un total de (préciser le type et le nombre de support(s) électronique(s)) , qui contiennent un listage de la ou des séquences ou un ou des tableaux y relatifs, déposés sous forme déchiffrable par ordinateur seulement, comme il est indiqué dans le cadre supplémentaire relatif au listage de la ou des séquences (voir l'instruction administrative 802).

4. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :
   - ☒ Cadre n° I Base de l'opinion
   - ☐ Cadre n° II Priorité
   - ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - ☐ Cadre n° IV Absence d'unité de l'invention
   - ☒ Cadre n° V Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - ☐ Cadre n° VI Certains documents cités
   - ☐ Cadre n° VII Irrégularités dans la demande internationale
   - ☐ Cadre n° VIII Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
20.04.2004	03.02.2005
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Barraco, G N° de téléphone +49 89 2399-2172

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

Demande internationale n°
PCT/FR 03/03309

Case No. I Base du rapport

1. En ce qui concerne la **langue**, le présent rapport est établi sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous ce point.

   ☐ Le présent rapport est établi sur la base de traductions réalisées à partir de la langue d'origine dans la langue suivante ,qui est la langue d'une traduction remise aux fins de :
   - ☐ la recherche internationale (selon les règles 12.3 et 23.1.b))
   - ☐ la publication de la demande internationale (selon la règle 12.4)
   - ☐ l'examen préliminaire international (selon la règle 55.2 ou 55.3)

2. En ce qui concerne les **éléments*** de la demande internationale, le présent rapport est établi sur la base des éléments suivants (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport.*) :

Description, Pages

1-26 telles qu'initialement déposées

Revendications, No.

1-41 reçue(s) le 20.04.2004 avec lettre du 16.04.2004

Dessins, Feuilles

1/6-6/6 telles qu'initialement déposées

☐ En ce qui concerne un listage de la ou des séquences ou un ou des tableaux y relatifs, voir le cadre supplémentaire relatif au listage de la ou des séquences.

3. ☐ Les modifications ont entraîné l'annulation :
   - ☐ de la description, pages
   - ☐ des revendications, nos
   - ☐ des dessins, feuilles/fig.
   - ☐ du listage de la ou des séquences *(préciser)* :
   - ☐ d'un ou de tous les tableaux relatifs au listage de la ou des séquences *(préciser)* :

4. ☐ Le présent rapport a été établi abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué dans le cadre supplémentaire (règle 70.2.c)).
   - ☐ de la description, pages
   - ☐ des revendications, nos
   - ☐ des dessins, feuilles/fig.
   - ☐ du listage de la ou des séquences *(préciser)* :
   - ☐ d'un ou de tous les tableaux relatifs au listage de la ou des séquences *(préciser)* :

** Si le cas visé au point 4 s'applique, certaines ou toutes ces feuilles peuvent être revêtues de la mention "remplacé".*

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

Demande internationale n°
PCT/FR 03/03309

Cadre n° V Déclaration motivée selon l?article 35.2) quant à la nouveauté, l?activité inventive et la possibilité d?application industrielle; citations et explications à l?appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-41
	Non:	Revendications	
Activité inventive	Oui:	Revendications	
	Non:	Revendications	1-41
Possibilité d'application industrielle	Oui:	Revendications	1-41
	Non:	Revendications	

2. Citations et explications (règle 70.7) :

voir feuille séparée

RAPPORT PRÉLIMINAIRE ITERNATIONAL SUR LA BREVETABILITÉ (FEUILLE SEPAREE)

Demande internationale n° PCT/FR 03/03309

Concernant le point V
Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence au document suivant:

D1: US-A-6 092 104 (KELLY CHRISTOPHER T) 18 juillet 2000 (2000-07-18)
D2: LASERVAULT UNIVERSAL SERVER ADDED FEATURES / BUG FIXES, [en ligne] 13 avril 1999 (1999-04-13) - 29 mars 2001 (2001-03-29), XP002182409 Extrait de l'Internet: <URL:http://laservault.com/support/whatIvu s.html> [extrait le 2001-11-09]
D3: EP-A-0 801 492 (MATSUSHITA ELECTRIC IND CO LTD) 15 octobre 1997 (1997-10-15)

2. D1 décrit un procédé d'analyse de la sécurité d'un système d'information comprenant une phase de modélisation du système d'information et un phase de simulation d'attaque potentielles contre le système d'information, du type définit dans la revendication 1 de la présente demande, voir D1: Introduction on pages 320-321 et le passage à la page 331.

L'objet de la revendication 1 diffère de l'état de la technique connu du document D1 en ce que la revendication précise que la modélisation est initialisée avec une valeur d'état de composant de système considérée "saine" et qui dans les cas d'attaque réussi l'état du composant passe à une valeur " non saine "

Or, bien que le document D1 ne mentionne pas le critère de " santé " de l'état pour juger la réussite de l'attaque, il est évident qui la considération de ce critère ne comporte pas des différences importantes au fonctionnement du procédé d'analyse de sécurité décrit dans la demande vis à vis du procédé d'analyse de sécurité décrit dans D1.

Il est aussi évident que dans la méthodologie de modélisation et simulation d'attaque décrite dans le document D1, la modélisation de relations entre les composants devrait tenir compte des relations de propagation susceptibles de véhiculer des attaques, voir à ce propos aussi les passages de la section 2 et 3 à les pages 321 et 322 de D1.

D'autre côte, la teneur de la revendication 1 ne spécifié pas quels prédicats ou actions sont compris dans les règles de comportement afin qu'une distinction soit possible lorsque on les compare avec les prédicats ou les actions des règles de comportements adoptées dans la méthodologie décrite dans D1.

Compte tenu des points ci-dessus combiner l'ensemble des caractéristiques exposées dans la revendication 1 relève d'une démarche technique normale pour la personne du métier. L'objet de la revendication 1 n'implique par conséquent pas d'activité inventive (article 33(3) PCT).

3. Les revendications dépendantes 2-38 ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, par ce que elles sont considérées comme caractéristiques opérationnelles évidentes pour un procède d'analyse de la sécurité d'un système d'information comme pour exemple le procède connue par D1.

4. Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document D1 et ne cite pas ce document, comme aussi les documents D2 et D3.

REVENDICATIONS

1. Procédé d'analyse de la sécurité d'un système d'information comprenant :

- une phase de modélisation (1,2), comprenant d'une part la spécification (1) de l'architecture du système d'information avec une représentation graphique d'un ensemble de composants du système et des relations entre lesdits composants, chaque composant étant associé à au moins un état initialisé avec une valeur saine, les relations entre deux composants déterminés comprenant des relations de propagation susceptibles de véhiculer des attaques, et d'autre part la spécification (2) d'un ensemble de règles de comportement, au plan du fonctionnement du système et au plan de la sécurité, associées aux composants du système, chaque règle de comportement comprenant un ou plusieurs prédicats et/ou une ou plusieurs actions; et,

- une phase de simulation, comprenant la spécification (3) et la simulation (4) d'attaques potentielles contre le système d'information, une attaque réussie faisant passer un état d'un composant à une valeur non saine.

2. Procédé selon la revendication 1, suivant lequel, un nom étant associé à chaque composant, un ou plusieurs adjectifs peuvent aussi être associés audit composant, lesquels adjectifs permettent de désigner ledit composant sans le nommer.

3. Procédé selon la revendication 1 ou la revendication 2, suivant lequel des états déterminés sont associés à chaque composant du système d'information, chaque état pouvant prendre une valeur saine et une ou plusieurs valeurs non saines.

4. Procédé selon la revendication 3, suivant lequel certains au moins desdits états se rapportent respectivement à l'activité, à la confidentialité, à l'intégrité et/ou à la disponibilité du composant auquel ils sont associés.

5. Procédé selon l'une quelconque des revendications précédentes, suivant lequel un nom prétendu peut être associé à un composant déterminé quelconque, notamment dans le cas où ledit composant déterminé est usurpateur.

6. Procédé selon l'une quelconque des revendications précédentes, suivant lequel un lien vers un autre composant peut être associé à un composant déterminé quelconque, notamment dans le cas où ledit composant déterminé est usurpé et où ledit autre composant est usurpateur.

7. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les relations de propagation sont des relations bidirectionnelles susceptibles de véhiculer des attaques dans les deux sens.

8. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les relations entre deux composants déterminés quelconques, comprennent des relations de service permettant de désigner un composant à partir d'un autre composant.

9. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les règles de comportement comprennent des règles de propagation d'attaques, ces règles étant par exemple mises en œuvre dans des composants qui sont des vecteurs d'attaques, et des règles d'absorption d'attaques, ces règles étant par exemple mise en œuvre dans des composants qui sont la cible d'attaques.

10. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les règles de comportement comprennent des règles binaires, par exemple des conditions logiques booléennes donnant une valeur de type oui / non, et/ou des règles fonctionnelles, par exemple des conditions logiques impliquant une action de routage (pour une règle de propagation) ou de contagion (pour une règle d'absorption).

11. Procédé l'une quelconque des revendications précédentes, comprenant, à la fin de la phase de modélisation (figure 3), la construction (35) d'une table de routage local, permettant de diriger une attaque d'un composant de départ vers un composant d'arrivée.

12. Procédé selon la revendication 11, suivant lequel la table de routage local est générée de façon automatique suivant le principe du plus court chemin entre le composant de départ et le composant d'arrivée.

13. Procédé selon l'une quelconque des revendications 3 à 12, suivant lequel l'étape de simulation des attaques comprend la mise à jour de l'état d'un composant du système altéré par une attaque réussie.

14. Procédé selon la revendication 13, suivant lequel la phase de simulation comprend en outre la constitution d'un fichier ou journal des attaques, contenant l'historique des changements de l'état des composants consécutifs à des attaques réussies, notamment pour permettre un traitement ultérieur par un utilisateur.

15. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les attaques comprennent des attaques élémentaires correspondant à des valeurs d'états non saines.

16. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les attaques comprennent en outre une attaque spéciale d'usurpation.

17. Procédé selon l'une quelconque des revendications précédentes, suivant lequel une attaque est définie, notamment, par un type d'attaque, un type de protocole, et des éléments de chemin d'attaque.

18. Procédé selon la revendication 17, suivant lequel les éléments de chemin d'attaque comprennent un composant de départ, un composant d'arrivée, un composant cible, et le cas échéant un ou plusieurs composants intermédiaires.

19. Procédé selon la revendication 17 ou la revendication 18, suivant lequel la liste des composants déjà traversés par une attaque est sauvegardée dans au moins une ou plusieurs piles amont.

20. Procédé selon la revendication 19, suivant lequel les pile amont comprennent une pile (110) contenant la liste exhaustive de tous les composants traversés, désignés par leur nom réel.

21. Procédé selon la revendication 19 ou la revendication 20, suivant lequel les piles amont comprennent une pile (120) contenant la liste des seuls composants traversés qui sont opaques, désignés par leur nom réel ou, le cas échéant, par leur nom prétendu.

22. Procédé selon l'une quelconque des revendications 17 à 21, suivant lequel la liste des composants destinataires d'une attaque est sauvegardée dans au moins une pile aval (130).

23. Procédé selon l'une quelconque des revendications précédentes, suivant lequel les attaques sont définies dans un langage utilisant les mêmes mots qu'un langage dans lequel les règles de comportement sont définies.

24. Procédé selon l'une quelconque des revendications précédentes, suivant lequel la phase de modélisation et/ou la phase de simulation sont mises en œuvre par un utilisateur au moyen d'une interface Homme/machine comportant une fonctionnalité multi vues, suivant laquelle une représentation graphique du système est présentée à l'utilisateur en plusieurs vues.

25. Procédé selon la revendication 24, suivant lequel chaque vue représente un sous-système du système, qui est relativement autonome et indépendant du reste du système.

26. Procédé selon la revendication 24 ou la revendication 25, suivant lequel la fonction d'interconnexion entre les composants compris dans deux vues distinctes est assurée seulement via le composant commun ou les composants communs aux deux vues.

27. Procédé selon l'une quelconque des revendications 24 à 26, suivant lequel les règles de comportement des composants appartenant à une vue ne font pas appel nommément à des composants appartenant à une autre vue.

28 Procédé selon l'une quelconque des revendications 24 à 27, suivant lequel les vues sont associées à des sous-systèmes respectifs, par exemple de même niveau, qui sont interconnectés entre eux via au moins un composant commun.

29. Procédé selon l'une quelconque des revendications 24 à 27, suivant lequel une vue supérieure est associée au système dans son ensemble, tandis qu'une ou plusieurs vues inférieures sont respectivement associées à un sous-système déterminé du système.

30. Procédé selon la revendication 29, suivant lequel un composant déterminé, commun à la vue supérieure et à une vue inférieure déterminée, représente le sous système correspondant vu du système dans son ensemble, et réciproquement.

31. Procédé selon la revendication 30, suivant lequel ledit composant commun est l'unique interface entre les la vue supérieure et ladite vue inférieure déterminée.

32. Procédé selon l'une quelconque des revendications précédentes, suivant lequel la phase de modélisation comprend en outre la spécification d'une ou plusieurs métriques de base respectivement associées aux composants.

33. Procédé selon la revendication 32, suivant lequel les métriques de base comprennent, une métrique d'efficacité des parades, une métrique d'efficacité de détection des attaques, et/ou une métrique des moyens d'un attaquant.

34. Procédé selon l'une quelconque des revendications précédentes, suivant lequel la phase de simulation comprend en le calcul d'une ou plusieurs métriques de probabilité de sinistre.

35. Procédé selon la revendication 34, suivant lequel les métriques de probabilité de sinistre comprennent une métrique de probabilité de passage d'une attaque sur un composant.

36. Procédé selon les revendications 32 et 34, suivant lequel la métrique de probabilité de passage d'une attaque sur un composant est calculée suivant la formule " probabilité de passage = (moyens de l'attaquant) / (efficacité de la protection)".

37. Procédé selon la revendication 34, suivant lequel les métriques de probabilité de sinistre comprennent une métrique de probabilité de non détection d'une attaque sur un composant.

38. Procédé selon les revendications 33 et 37, suivant lequel la métrique de probabilité de non détection d'une attaque sur un composant est calculée suivant la formule "probabilité de non détection = (moyens de l'attaquant) / (efficacité de la détection)".

39. Dispositif pour la mise en œuvre d'un procédé selon l'une quelconque des revendications précédentes, comprenant une interface Homme / machine (15) pour la mise en œuvre de la phase de modélisation et/ou un moteur attaques / parades (16) pour la mise en œuvre de la phase de simulation

40. Dispositif selon la revendication 39, dans lequel l'interface Homme / machine présente une fonctionnalité d'affichage en multi vues du système modélisé.

41. Dispositif selon la revendication 39 ou la revendication 40, dans lequel l'interface Homme / machine permet d'afficher le système modélisé selon un modèle composants / relations.